

09/037797

J002 H0015-07/910 2 8 SEP 2001

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: KANEMAKI, H. et al

Serial No.: not yet assigned

Filed: September 28, 2001

For: Authentication Apparatus, Authentication System, and Method of Same, Processing Apparatus, Communication Apparatus, Communication control Apparatus, Communication System, and Method of Same, Information Storage Method and Apparatus of Same, Information Restoration Method and Apparatus of Same, and Storage Medium of Same

Case No.: 9798423-0007

Group Art Unit: not yet assigned

Examiner: not yet assigned

Date: September 28, 2001

Express Mail Label No. EL676986655US

Certificate of Express Mailing (37 CFR 1.10)

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as U.S. Express Mail in an envelope addressed to:

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231, on:

Date of Deposit: September 28, 2001

Paula M. Theismann 92801
Paula M. Theismann Date

PRELIMINARY AMENDMENT ACCOMPANYING APPLICATION

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Please amend the accompanying application as follows:

In the Specification

On page 1, line 11, change "TECHNICAL FIELD" to --BACKGROUND OF THE INVENTION--;

On page 5, line 23, change, "DISCLOSURE OF THE INVENTION" to --SUMMARY OF THE INVENTION--;

A clean copy of the amended headings is included with this Preliminary Amendment.

In the Claims:

Claims 2-3, 6, 11, 17-18, 20-23, 34-36, 42-44, 49-55, 63-72, 74-80, 88, 96-99, 114-119, 137, 153-154, 159-161, 165, have been cancelled.

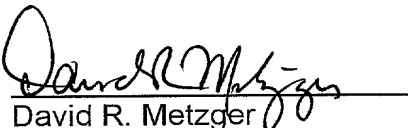
The claims have been renumbered 1-116.

Replacement pages of the renumbered claims 1-116 are attached as well as a marked-up version showing the cancellation of the above-identified claims.

Respectfully submitted,

SONNENSCHN NATH & ROSENTHAL

SONNENSCHN NATH & ROSENTHAL
P.O. Box 061080
Wacker Drive Station - Sears Tower
Chicago, Illinois 60606-1080
Telephone: (312) 876-8000

By: 
David R. Metzger
Registration No. 32,919

205110 666666

Clean Copy of Corrected Specification Headings

In the specification:

Page 1, line 11, change "TECHNICAL FIELD" to --BACKGROUND OF THE INVENTION--

BACKGROUND OF THE INVENTION

Page 5, line 23, change "DISCLOSURE OF THE INVENTION" to --SUMMARY OF THE INVENTION--

SUMMARY OF THE INVENTION

- 1 -

CLAIMS

1. An authentication apparatus for authenticating a transaction performed between at least two parties via a network,

5 said authentication apparatus comprising:

a first receiving means for receiving a first request including personal key information of a first transactor and information indicating a transaction content from said first transactor,

10 a first authenticating means for authenticating a legitimacy of said first transactor based on said personal key information included in said first request and generating first authentication information,

15 a first transmitting means for transmitting a second request including information obtained by deleting the personal key information of said first transactor from said first request and said first authentication information to said second transactor,

20 a second receiving means for receiving a reply with respect to said second request from said second transactor,

a second authenticating means for authenticating the legitimacy of said second transactor and generating second authentication information in
25 accordance with said reply, and

a second transmitting means for transmitting said second authentication information to said first transactor.

2. An authentication system for authenticating a transaction performed between at least two parties via a network,

said authentication system comprising:

a first communication apparatus used by a first transactor,

10 a second communication apparatus used by a second transactor, and

an authentication apparatus for authenticating said transaction,

wherein

15 said authentication apparatus comprises

a first receiving means for receiving a first request including personal key information of the first transactor and information indicating transaction content from said first transactor,

20 a first authenticating means for authenticating a legitimacy of said first transactor based on said personal key information included in said first request and generating first authentication information,

a first transmitting means for transmitting a
25 second request including information obtained by deleting

the personal key information of said first transactor
from said first request and said first authentication
information to said second transactor,

a second receiving means for receiving a reply
5 with respect to said second request from said second
transactor,

a second authenticating means for
authenticating the legitimacy of said second transactor
and generating second authentication information in
10 accordance with said reply, and

a second transmitting means for transmitting
the second authentication information indicating the
legitimacy of said transaction to said first transactor.

3. An authentication method for authenticating a
15 transaction performed between at least two parties via a
network,

said authentication method comprising the steps
of:

receiving a first request including personal
20 key information of a first transactor and information
indicating transaction content from said first
transactor,

authenticating a legitimacy of said first
transactor based on said personal key information
25 included in said first request and generating first

authentication information,

transmitting a second request including
information obtained by deleting the personal key

information of said first transactor from said first

5 request and said first authentication information to said
second transactor,

receiving a reply with respect to said second
request from said second transactor,

authenticating a legitimacy of said second
10 transactor in accordance with said reply and generating
second authentication information, and

transmitting said second authentication
information to said first transactor.

4. An authentication apparatus for authenticating
15 a transaction performed between at least two parties via
a network,

said authentication apparatus comprising:

a first receiving means for receiving a first
request including personal identification information of
20 a first transactor and information indicating transaction
content from said first transactor,

a first authenticating means for authenticating
a legitimacy of said first transactor and generating a
first authentication information in response to said
25 first request,

5 a second receiving means for receiving a reply
with respect to said second request from said second
transactor,

a second transmitting means for transmitting said second authentication information to said first transactor.

said first receiving means receives said first request further including the personal key information of said first transactor, and

6. An authentication apparatus as set forth in claim 5, wherein said personal key information of said first transactor is information relating to the charging

of said first transactor.

7. An authentication apparatus as set forth in claim 6, wherein said first transmitting means transmits the second request further including said personal key information of said first transactor to said second transactor.

8. An authentication apparatus as set forth in claim 4, further comprising a decrypting means for decrypting said received first request when said first request is encrypted.

9. An authentication apparatus as set forth in claim 4, further comprising an encrypting means for encrypting said second request.

10. An authentication apparatus as set forth in claim 4, further comprising a decrypting means for decrypting said received reply when said reply is encrypted.

11. An authentication apparatus as set forth in claim 4, further comprising an encrypting means for encrypting said second authentication information.

12. An authentication system for authenticating a transaction performed between at least two parties via a network,

said authentication system comprising:

a first communication apparatus used by a first

transactor,

a second communication apparatus used by a
second transactor, and

an authentication apparatus for authenticating
5 said transaction,

wherein

said first communication apparatus transmits a
first request including personal identification
information of the first transactor and information
10 indicating the transaction content to said authentication
apparatus, and

said authentication apparatus comprises:

a first receiving means for receiving said
first request from said first transactor,

15 a first authenticating means for authenticating
a legitimacy of said first transactor and generating
first authentication information in response to said
first request,

a first transmitting means for transmitting a
20 second request including said first authentication
information and the content of said transaction to said
second transactor,

a second receiving means for receiving a reply
with respect to said second request from said second
25 transactor,

a second authenticating means for authenticating a legitimacy of said second transactor and generating second authentication information in response to said reply, and

5 a second transmitting means for transmitting said second authentication information to said first transactor.

13. An authentication method for authenticating a transaction performed between at least two parties via a
10 network,

said authentication method comprising the steps of:

receiving a first request including personal identification information of a first transactor and
15 information indicating transaction content from said first transactor,

authenticating a legitimacy of said first transactor and generating first authentication information in response to said first request,

20 transmitting a second request including said first authentication information and the content of said transaction to a second transactor,

receiving a reply with respect to said second request from said second transactor,

25 authenticating a legitimacy of said second

20257410 46446660

transactor in accordance with said reply and generating second authentication information, and

transmitting said second authentication information to said first transactor.

5 14. An authentication apparatus holding information relating to a first transactor and authenticating a transaction between said first transactor and a second transactor performed via a network while communicating with another authentication apparatus holding information
10 relating to said second transactor,

said authentication apparatus comprising:

a transmitting and receiving means for transmitting a second request including information specifying said second transactor in response to a first
15 request from said first transactor including information indicating said transaction content and information specifying said second transactor to said second authentication apparatus, receiving first signature information indicating an authentication result by said
20 second authentication apparatus in response to said second request, transmitting a third request including information relating to said transaction content included in said first request and said first signature information to an apparatus used by said second
25 transactor, and receiving a predetermined reply from an

apparatus used by said second transactor in response to the related third request,

a storage means for storing a log of said transaction when receiving said predetermined reply, and

5 a signature producing means for producing second signature information to be transmitted to the apparatus used by said first transactor via said transmitting and receiving means when receiving said predetermined reply and indicating the authentication
10 result of the legitimacy of said transaction.

15. An authentication apparatus as set forth in claim 14, further comprising an encrypting means, and wherein

said transmitting and receiving means receives
15 an encryption key used for the communication with said second transactor from said other authentication apparatus in response to said second request and transmits the information relating to said transaction content encrypted by using said encryption key at said
20 encrypting means and said first signature information to the apparatus used by said second transactor.

16. An authentication apparatus as set forth in claim 14, wherein

said transmitting and receiving means receives
25 said predetermined reply including the identification

information used for identifying said second transactor by said other authentication apparatus from the apparatus used by said second transactor, and

said storage means stores a log of said
5 transactions generated by using said identification information.

17. An authentication apparatus as set forth in claim 14, wherein said transmitting and receiving means transmits the third request including information other
10 than the information relating to the charging of said first transactor in the information relating to said transaction content included in said first request and said first signature information to the apparatus used by said second transactor.

15 18. An authentication apparatus as set forth in claim 14, wherein said transmitting and receiving means transmits the third request including the information relating to said transaction content included in said first request, said first signature information, and the
20 encryption key used for the communication with the related authentication apparatus to the apparatus used by said second transactor.

19. An authentication apparatus as set forth in claim 14, further comprising a charge processing means
25 for the charge processing for the authentication relating

to said transaction.

20. An authentication apparatus as set forth in claim 14, wherein said charge processing means performs processing for determining a rate of the charge for the authentication relating to said transaction with said
5 other authentication apparatus.

21. An authentication apparatus as set forth in claim 14, wherein said transmitting and receiving means receives said predetermined reply from the apparatus used
10 by said second transactor when said second transactor confirms the legitimacy of said first signature information and agrees to the related transaction.

22. An authentication apparatus as set forth in claim 14, wherein said receiving means sends said second
15 signature information to the apparatus used by said second transactor.

23. An authentication system for authenticating a transaction performed between at least two parties via a network,

20 said authentication system comprising:

a first authentication apparatus for authenticating a transaction relating to a first transactor and

a second authentication apparatus for
25 authenticating a transaction relating to a second

transactor,

wherein

2057110 2626560

said first authentication apparatus transmits a second request including information specifying said second transactor to said second authentication apparatus in response to a first request by said first transactor including information indicating said transaction content and information specifying said second transactor, receives first signature information from said second authentication apparatus in response to said second request, transmits a third request including information relating to said transaction content included in said first request and said first signature information to the apparatus used by said second transactor, stores a log of said transaction when receiving a predetermined reply from said second transactor in response to the related third request, and provides second signature information for authenticating a legitimacy of said transaction to said first transactor.

20 24. An authentication method for authenticating a transaction between a first transactor and a second transactor performed via a network by using a first authentication apparatus for authenticating a transaction relating to the first transactor and a second authentication apparatus for authenticating a transaction

relating to the second transactor,

said authentication method comprising the steps
of:

issuing a first request including information
5 indicating said transaction content and information
specifying said second transactor from said first
transactor to said first authentication apparatus,

transmitting a second request including the
information specifying said second transactor from said
10 first authentication apparatus to said second
authentication apparatus in response to said first
request,

transmitting first signature information
indicating the authentication result by the related
15 second authentication apparatus to said first
authentication apparatus from said second authentication
apparatus in response to said second request,

transmitting a third request including the
information relating to said transaction content included
20 in said first request and said first signature
information from said first authentication apparatus to
an apparatus used by said second transactor,

issuing a predetermined reply from the
apparatus used by said second transactor to said first
25 authentication apparatus in response to the related third

20257140 4642560

request and,

in accordance with said predetermined reply,
storing a log of said transaction, producing second
signature information indicating the authentication
5 result of the legitimacy of said transaction, and
transmitting the related second signature information to
the apparatus used by said first transactor by said first
authentication apparatus.

25. An authentication method as set forth in claim
10 24, further comprising the steps of:

sending an encryption key for use in
communication with said second transactor from said
second authentication apparatus to said first
authentication apparatus in accordance with said second
15 request and

having said first authentication apparatus
encrypt said information relating to transaction content
and said first signature information using said
encryption key, then send them to the apparatus used by
20 said second transactor.

26. An authentication method as set forth in claim
24, further comprising the steps of having said first
authentication apparatus receive said predetermined reply
including identification information for use by said
25 second authentication apparatus in identifying said

second transactor from the apparatus used by said second transactor and store a log of said transaction generated using said identification information.

27. An authentication method as set forth in claim
5 24, further comprising the steps of sending a third request including information other than the information relating to the charging of said first transactor in the information relating to said transaction content included in said first request and said first signature
10 information from the first authentication apparatus to the apparatus used by said second transactor.

28. An authentication method as set forth in claim
24, further comprising the steps of sending a third request including information relating to the charging of
15 said first transactor included in said first request, said first signature information, and an encryption key for use in communication with said authentication apparatus from the first authentication apparatus to the apparatus used by said second transactor.

29. An authentication method for authenticating a
20 transaction between a first transactor and a second transactor performed via a network by using a first authentication apparatus for authenticating a transaction relating to the first transactor and a second
25 authentication apparatus for authenticating a transaction

relating to the second transactor,

said authentication method comprising the steps
of:

- issuing a first request including information
- 5 indicating said transaction content, personal key
information of said first transactor, and information
specifying said second transactor from said first
transactor to said first authentication apparatus,
- transmitting a second request obtained by
- 10 deleting said personal key from said first request from
said first authentication apparatus to said second
authentication apparatus in response to said first
request,
- transmitting a third request including
- 15 information indicating the content of said transaction
from said second authentication apparatus to the
apparatus used by said second transactor in response to
said second request,
- transmitting a first reply from the apparatus
- 20 used by said second transactor to said second
authentication apparatus in response to said third
request,
- transmitting a second reply including payment
method information indicating a payment method to said
- 25 second transactor from said second authentication

20251110 16:26:56

apparatus to said first authentication apparatus in
accordance with said first reply, and

managing a payment relating to said transaction
between said first transactor and said second transactor
5 based on said payment method information by said first
authentication apparatus.

30. An authentication method as set forth in claim
29, wherein said first authentication apparatus performs
processing for receiving a payment from said first
10 transactor relating to said transaction, processing for
paying a part of said payment to said second transactor
in accordance with said transaction, and processing for
receiving a remainder of said payment as a fee.

31. An authentication method as set forth in claim
15 29, wherein said first authentication apparatus inquires
to said second authentication apparatus whether or not
said second transactor has contracted with said second
authentication apparatus in response to said first
request and, when receiving an answer indicating it has
20 contracted with it from said second authentication
apparatus, transmits said second request to said second
authentication apparatus.

32. An authentication method as set forth in claim
29, wherein when receiving said second reply, said first
25 authentication apparatus transmits a third reply

2025110 16446660

including signature information including the result of authentication performed by the related first authentication apparatus for said transactor to the apparatus used by said first transactor.

5 33. An authentication apparatus holding information relating to a first transactor and authenticating a transaction between said first transactor and a second transactor performed via a network while communicating with another authentication apparatus holding information
10 relating to said second transactor,

 said authentication apparatus comprising:

 a receiving means for receiving a first request including information indicating said transaction content, personal key information of said first
15 transactor, and information specifying said second transactor from said first transactor and receiving a reply including payment method information indicating a payment method to said second transactor from said other authentication apparatus,

20 a transmitting means for transmitting a second request obtained by deleting said personal key from said first request to said other authentication apparatus in response to said first request, and

 a charging means for managing a payment
25 relating to said transaction between said first

transactor and said second transactor based on said payment method information.

34. An authentication apparatus as set forth in claim 33, wherein said charging means performs processing
5 for receiving a payment from said first transactor relating to said transaction, processing for paying a part of said payment to said second transactor in accordance with said transaction, and processing for receiving a remainder of said payment as a fee.

10 35. An authentication apparatus as set forth in claim 33, wherein said transmitting means inquires to said other authentication apparatus whether or not said second transactor has contracted with said second authentication apparatus in response to said first
15 request and, when receiving an answer indicating it has contracted with it from said other authentication apparatus, transmits said second request to said other authentication apparatus.

36. An authentication apparatus as set forth in
20 claim 33, wherein when said receiving means receives said second reply, said transmitting means transmits a reply including signature information including the result of authentication performed by itself for said transactor to the apparatus used by said first transactor.

25 37. An authentication apparatus as set forth in

claim 36, wherein said transmitting means encrypts said reply by using a secret key corresponding to the related first authentication apparatus and transmits the same to the apparatus used by said first transactor.

5 38. An authentication apparatus as set forth in claim 33, wherein said transmitting means transmits said second request further including the signature information indicating the result of authentication performed by the related first authentication apparatus
10 for said transaction to said other authentication apparatus.

 39. An authentication system comprising a first authentication apparatus for authenticating a transaction relating to a first transactor and a second
15 authentication apparatus for authenticating a transaction relating to a second transactor and authenticating a transaction between said first transactor and said second transactor performed via a network,

 said authentication system comprising the steps
20 of:

 issuing a first request including information indicating said transaction content, personal key information of said first transactor, and information specifying said second transactor from said first
25 transactor to said first authentication apparatus,

transmitting a second request obtained by deleting said personal key from said first request from said first authentication apparatus to said second authentication apparatus in response to said first request,

transmitting a third request including the information indicating the content of said transaction from said second authentication apparatus to the apparatus used by said second transactor in response to said second request,

transmitting a first reply from an apparatus used by said second transactor to said second authentication apparatus in response to said third request,

transmitting a second reply including payment method information indicating a payment method to said second transactor from said second authentication apparatus to said first authentication apparatus in accordance with said first reply, and

managing a payment relating to said transaction between said first transactor and said second transactor based on said payment method information by said first authentication apparatus.

40. An authentication method comprising the steps of:

having an authentication apparatus divide authentication information of a user into first authentication information and second authentication information,

5 providing a portable memory device storing said second authentication information to said user,

transmitting an authentication information request from a terminal capable of accessing said portable memory device to said authentication apparatus,

10 transmitting said first authentication information from said authentication apparatus to said terminal when said authentication apparatus decides said authentication information request is by a legitimate user, and

15 having said terminal restore said authentication information by using said first authentication information received from said authentication apparatus and said second authentication information read from said portable memory device.

20 41. An authentication method comprising the steps of:

generating authentication information,

dividing said authentication information into first authentication information and second

25 authentication information,

providing a portable memory device storing said
second authentication information to a user, and

transmitting said first authentication
information to a transmission destination designated by
5 said authentication information request when deciding
that the received authentication information request is
by a legitimate user.

42. An authentication method as set forth in claim
41, further comprising the steps of:

10 storing in advance transmission destination
information corresponding to the user and

deciding that said authentication information
request is by a legitimate user when said transmission
destination information included in said authentication
15 information request is present in said stored
transmission destination information. .

43. An authentication method as set forth in claim
41, wherein said authentication information is
information produced using public key encryption.

20 44. An authentication method as set forth in claim
41, wherein said portable memory device is a smart card.

45. An authentication apparatus comprising:
a controlling means for generating
authentication information, dividing said authentication
25 information into first authentication information and

second authentication information, and deciding whether
or not the received authentication information request is
by a legitimate user,

a writing means for writing said second
5 authentication information into a portable memory device,

a receiving means for receiving said
authentication information request from a user of said
portable memory device, and

a transmitting means for transmitting said
10 first authentication information to a transmission
destination designated by said authentication information
request when it is decided that said authentication
information request is by a legitimate user.

46. An authentication apparatus as set forth in
15 claim 45, further comprising

a storage means for storing in advance
transmission destination information corresponding to the
user is further provided and

wherein

20 said controlling means decides that said
authentication information request is by a legitimate
user when said transmission destination information
included in said authentication information request is
present in said stored transmission destination
25 information.

09937797-041500

47. An authentication apparatus as set forth in claim 45, wherein said authentication information is information produced using public key encryption.

48. A communication apparatus comprising:

5 a receiving means for receiving a request including personal identification information for identifying a user,

 a storage means for storing said personal identification information and information of a
10 transmission destination for transmitting a processing result in correspondence,

 a processing means for performing predetermined processing in response to said request, and

 a transmitting means for reading information of
15 said transmission destination corresponding to said personal identification information included in said request from said storage means and transmitting the result of said processing to the transmission destination specified by the related read information of said
20 transmission destination.

49. A communication apparatus as set forth in claim 48, wherein

 said receiving means receives a request including encrypted personal identification information,
25 and

said communication apparatus further comprises a decrypting means for decrypting said personal identification information included in said received request.

5 50. A communication apparatus as set forth in claim 48, wherein said personal identification information is an identifier assigned to the user registered in the communication apparatus in advance.

10 51. A communication apparatus as set forth in claim 48, wherein the information of the transmission destination for transmitting the result of said processing is information provided by the transmitting side of said request to the related communication apparatus off-line.

15 52. A communication apparatus as set forth in claim 48, wherein the information of the transmission destination for transmitting said predetermined result is personal identification information for unambiguously identifying said user in the network with the related communication apparatus connected thereto.

 53. A communication apparatus as set forth in claim 48, wherein said processing is authentication processing.

 54. A communication system comprising
 a first communication apparatus and
25 a second communication apparatus connected via

205710-26245500

a network, wherein

said first communication apparatus comprises:

a first receiving means for receiving a request including personal identification information for

5 identifying a user,

a storage means for storing said personal identification information and information of a transmission destination for transmitting a processing result in correspondence,

10 a processing means for performing predetermined processing in response to said request, and

a first transmitting means for reading the information of said transmission destination corresponding to said personal identification information included in said request from said storage means and transmitting the result of said processing to the transmission destination specified by the related read information of said transmission destination and wherein

15 said second communication apparatus comprises:

20 a second transmitting means for transmitting said request to said first communication apparatus,

a second receiving means for receiving the result of said processing from said first communication apparatus, and

25 an outputting means for outputting the result

of the related received authentication processing.

55. A communication method using a first communication apparatus and a second communication apparatus connected via a network,

5 said communication method comprising the steps of:

 transmitting a request including personal identification information for identifying a user from said second communication apparatus to said first
10 communication apparatus,

 having said first communication apparatus perform predetermined processing in response to said request, and

 having said first communication apparatus refer
15 to a correspondence of said personal identification information and information of a transmission destination for transmitting the result of the processing produced in advance and transmit a result of said processing to the transmission destination specified by information of the
20 transmission destination corresponding to said personal identification information included in said request.

56. A communication method as set forth in claim 55, further comprising the step of having said second communication apparatus output the results of said
25 processing received from said first communication

apparatus.

57. A communication method as set forth in claim
55, further comprising the step of having said first
communication apparatus receive said request including
5 encrypted personal identification information and decrypt
said personal identification information included in said
received reply.

58. A communication method as set forth in claim
55, wherein said personal identification information is
10 an identifier assigned to a user registered at said first
communication apparatus in advance.

59. A communication method as set forth in claim
55, wherein the information of the transmission
destination for transmitting the result of said
15 processing is information provided by the transmitting
side of said request to the related first communication
apparatus off-line.

60. A communication method as set forth in claim
55, wherein the information of the transmission
20 destination for transmitting said predetermined result is
personal identification information for unambiguously
identifying said user in the network with the related
first communication apparatus connected thereto.

61. An authentication apparatus for authenticating
25 a transaction performed between at least two parties via

a network,

said authentication apparatus comprising:

a first receiving means for receiving a first
request including personal key information of a first
5 transactor and information indicating a transaction
content from said first transactor,

a first authenticating means for authenticating
a legitimacy of said first transactor based on said
personal key information included in said first request
10 and generating first authentication information,

a first transmitting means for transmitting a
second request including information obtained by deleting
the personal key information of said first transactor
from said first request and including said first
15 authentication information to a second transactor,

a second receiving means for receiving a reply
with respect to said second request from said second
transactor,

a second authenticating means for
20 authenticating a legitimacy of said second transactor and
generating second authentication information,

a second transmitting means for transmitting
said second authentication information to said first
transactor,

25 an identification information issuing means for

issuing transaction identification information when
receiving said first request, and

a log managing means for managing a log of the
reception of said first request, transmission of said
5 second request, and the reception of said reply by using
said transaction identification information.

62. An authentication apparatus as set forth in
claim 61, wherein said transaction log managing means
generates log information for each of the reception of
10 said first request, transmission of said second request,
and reception of said reply and stores the related log
information relating to said transaction identification
information.

63. An authentication apparatus as set forth in
15 claim 61, wherein said transmitting means transmits a
second request further including said transaction
identification information to said second transactor.

64. An authentication apparatus as set forth in
claim 63, wherein said second authenticating means
20 authenticates the legitimacy of said reply based on said
transaction identification information included in said
reply and said log managed by said transaction log
managing means.

65. An authentication apparatus as set forth in
25 claim 61,

further comprising an account processing means for performing the account processing concerned in said transaction, and

wherein

5 said transaction log managing means stores log information indicating that the account processing is terminated in correspondence with said transaction identification information after the end of said account processing.

10 66. An authentication apparatus as set forth in claim 61, wherein the personal key information of said first transactor is information relating to the charging of said first transactor.

15 67. An authentication system for authenticating a transaction performed between at least two parties via a network,

 said authentication system comprising

 a first communication apparatus used by a first transactor,

20 a second communication apparatus used by a second transactor, and

 an authentication apparatus for authenticating said transaction, wherein

 said authentication apparatus comprises:

25 a first receiving means for receiving a first

request including personal key information of said first transactor and including an information indicating the transaction content from said first transactor,

5 a first authenticating means for authenticating a legitimacy of said first transactor based on said personal key information included in said first request and generating first authentication information,

10 a first transmitting means for transmitting a second request including information obtained by deleting the personal key information of said first transactor from said first request and including said first authentication information to said second transactor,

15 a second receiving means for receiving a reply with respect to said second request from said second transactor,

a second authenticating means for authenticating a legitimacy of said second transactor in accordance with said reply and generating second authentication information,

20 a second transmitting means for transmitting said second authentication information to said first transactor,

a transaction identification information issuing means for issuing transaction identification information when receiving said first request, and

25

a transaction log managing means for managing a log of the reception of said first request, transmission of said second request, and the reception of said reply by using said transaction identification information.

5 68. An authentication method for authenticating a transaction performed between at least two parties via a network,

said authentication method comprising the steps of:

10 receiving a first request including personal key information of a first transactor and including information indicating a transaction content from said first transactor,

15 issuing transaction identification information in accordance with the related reception,

authenticating a legitimacy of said first transactor based on said personal key information included in said first request and generating first authentication information,

20 transmitting a second request including information obtained by deleting the personal key information of said first transactor from said first request and including said first authentication information to said second transactor,

25 receiving a reply with respect to said second

request from said second transactor,

authenticating a legitimacy of said second
transactor in accordance with said reply and generating
second authentication information,

5 transmitting said second authentication
information to said first transactor, and

managing a log of the reception of said first
request, transmission of said second request, and the
reception of said reply by using said transaction log
10 information.

69. A communication control apparatus for
controlling communication processing carried out in a
second communication apparatus on a network in response
to a request from one or more first communication
15 apparatuses,

said communication control apparatus
comprising:

a storage means for storing apparatus
identification information for identifying said first
20 communication apparatus,

a transmitting means for transmitting a request
including said apparatus identification information
corresponding to the related first communication
apparatus to said second communication apparatus in
25 response to the request from said first communication

apparatus,

a receiving means for receiving a reply
including the apparatus identification information for
identifying the transmitting apparatus of said request
5 from said second communication apparatus, and

a controlling means for deciding if said
request corresponding to said received reply is by a
legitimate first communication apparatus whose apparatus
identification information is stored in said storage
10 means based on whether or not said apparatus
identification information included in said reply and
said apparatus identification information stored in said
storage means coincide.

70. A communication control apparatus as set forth
15 in claim 69, wherein said controlling means sends a
predetermined notification to said second communication
apparatus when said apparatus identification information
included in said reply and said apparatus identification
information stored in said storage means do not coincide.

71. A communication control apparatus as set forth
20 in claim 69, wherein said controlling means sends a
predetermined notification to an apparatus of the
destination of a transaction where the result of
processing included in said reply is used when said
25 apparatus identification information included in said

09937797 011502
205710 26225660

reply and said apparatus identification information stored in said storage means do not coincide.

72. A communication control apparatus as set forth in claim 69, wherein said transmitting means transmits
5 said request including personal identification information received from said first communication apparatus and including said apparatus identification information corresponding to the related first communication apparatus to said second communication
10 apparatus.

73. A communication control apparatus as set forth in claim 69, wherein said storage means stores said apparatus identification information received from said first communication apparatus.

15 74. A communication control apparatus as set forth in claim 73, wherein said storage means stores said apparatus identification information received from said first communication apparatus when a power of the related communication control apparatus is turned on.

20 75. A communication control apparatus as set forth in claim 69, wherein said controlling means writes a communication log between said first communication apparatus and said second communication apparatus in said storage means.

25 76. A communication control apparatus as set forth

in claim 69, wherein said controlling means transmits the processing result of said second communication apparatus included in said reply to said first communication apparatus of the transmission destination of said request.

77. A communication control apparatus as set forth in claim 69, wherein said controlling means controls the communication so that said first communication apparatus in a stand-by state enters an operating state in accordance with the information received from said receiving means.

78. A communication control apparatus as set forth in claim 69, wherein said controlling means controls the communication between a network to which said first communication apparatus is connected and a network to which said second communication apparatus is connected.

79. A communication control apparatus as set forth in claim 69, wherein said controlling means performs processing as a gateway.

80. A communication control apparatus as set forth in claim 69, wherein said apparatus identification information is an identifier that can unambiguously identify the related communication apparatus assigned by the manufacturer of said first communication apparatus.

81. A communication control apparatus as set forth

in claim 69, wherein said personal identification information is an identifier assigned to a registered user in advance.

82. A communication control apparatus as set forth
5 in claim 69, wherein said receiving means receives said reply including the result of authentication processing performed by said second communication apparatus from said second communication apparatus.

83. A communication system for controlling at a
10 communication control apparatus communication relating to processing carried out at a second communication apparatus on a network in response to a request from one or more first communication apparatuses, wherein

said communication control apparatus comprises:

15 a first storage means for storing apparatus identification information for identifying said first communication apparatus,

a first transmitting means for transmitting a request including said apparatus identification
20 information corresponding to the related first communication apparatus and including personal identification information to said second communication apparatus in response to the request from said first communication apparatus,

25 a first receiving means for receiving a reply

including the apparatus identification information for identifying the transmitting apparatus of said request from said second communication apparatus, and

5 a controlling means for deciding if said request corresponding to said received reply is by a legitimate first communication apparatus whose apparatus identification information is stored in said first storage means based on whether or not said apparatus identification information included in said reply and
10 said apparatus identification information stored in said first storage means coincide and wherein
said second communication apparatus comprises:
a second receiving means for receiving said request,
15 a second storage means for storing said request,
a second storage means for storing said personal identification information and information of a transmission destination for transmitting a processing
20 result in correspondence,
a processing means for performing predetermined processing in response to said request, and
a second transmitting means for reading the information of said transmission destination
25 corresponding to said personal identification information

included in said request from said second storage means
and transmitting the result of said processing and said
apparatus identification information included in said
request in correspondence to the transmission destination
5 specified by the related read transmission destination
information.

84. A communication method for controlling at the
communication control apparatus communication relating to
processing carried out at a second communication
10 apparatus on a network in response to a request from one
or more first communication apparatuses,

said communication method comprising the steps
of:

transmitting a request including apparatus
15 identification information corresponding to the related
first communication apparatus and including personal
identification information from said communication
control apparatus to said second communication apparatus
in response to the request issued from said first
20 communication apparatus to said communication control
apparatus,

having said second communication apparatus
perform predetermined processing in response to said
received request,

25 having said second communication apparatus

transmit a reply including the result of said processing
and including said apparatus identification information
included in said request to said communication control
apparatus based on the information of the transmission
5 destination corresponding to said personal identification
information included in said request, and

having said communication control apparatus
decide if said request corresponding to said received
reply is by a legitimate first communication apparatus
10 based on whether or not said apparatus identification
information included in said received reply and said
apparatus identification information of said first
communication apparatus held in advance coincide.

85. A communication method as set forth in claim
15 84, wherein said communication control apparatus sends a
predetermined notification to said second communication
apparatus when said apparatus identification information
included in said received reply and said apparatus
identification information of said first communication
20 apparatus held in advance do not coincide.

86. An authentication apparatus for performing
authentication processing in response to an
authentication request,

said authentication apparatus comprising:
25 a receiving means for receiving said

authentication request including personal identification information for identifying a user and including apparatus identification information for identifying a transmitting apparatus of said authentication request,

5 a storage means for storing said personal identification information and the information of the transmission destination for transmitting an authentication result in correspondence,

10 an authentication processing means for performing authentication processing in response to said authentication request, and

15 a transmitting means for reading the information of said transmission destination corresponding to said personal identification information included in said authentication request from said storage means and transmitting the result of said authentication processing and said apparatus identification information included in said authentication request in correspondence to the transmission destination specified by the related read transmission destination information.

20

87. An authentication apparatus as set forth in claim 86, wherein

25 said receiving means receives said authentication request including encrypted personal identification information and apparatus identification

information, and

said authentication apparatus further comprises
a decrypting means for decrypting said personal
identification information and said apparatus
5 identification information included in said received
authentication request.

88. An authentication apparatus as set forth in
claim 86, wherein said receiving means receives said
authentication request further including third
10 identification information used for the charge processing
relating to said user.

89. An authentication apparatus as set forth in
claim 86, wherein said personal identification
information is an identifier assigned to a registered
15 user in advance.

90. An authentication apparatus as set forth in
claim 86, wherein said apparatus identification
information is an identifier capable of unambiguously
identifying the related apparatus assigned by the
20 manufacturer of said apparatus.

91. An authentication apparatus for performing
authentication processing relating to a transaction
performed via a network,

said authentication apparatus comprising:
25 a receiving means for receiving an

authentication request by a user engaging in a
transaction including personal identification information
for identifying the user, transaction information
indicating content of the transaction, and apparatus
5 identification information for identifying a transmitting
apparatus of said authentication request,

a storage means for storing said personal
identification information and information of a
transmission destination for transmitting the
10 authentication result in correspondence,

an authentication processing means for
transmitting said transaction information included in
said received authentication request to an apparatus of
the user designated by said authentication request and
15 performing predetermined authentication processing in
accordance with a reply from the apparatus of the related
designated user, and

a transmitting means for reading the
information of said transmission destination
20 corresponding to said personal identification information
included in said authentication request from said storage
means and transmitting the result of said authentication
processing and said apparatus identification information
included in said authentication request in correspondence
25 to the transmission destination specified by the related

read transmission destination information.

92. An authentication apparatus as set forth in claim 91, wherein said authentication processing means attaches signature information indicating the authentication result of the related authentication apparatus to said transaction information and transmits the same to the apparatus of said designated user and generates signature information of the related authentication apparatus of the result of said authentication processing in accordance with the reply from said designated user.

93. An authentication apparatus as set forth in claim 91, wherein said storage means stores log information of transactions between the user issuing said authentication request and said designated user.

94. An authentication apparatus as set forth in claim 91, wherein
said receiving means receives said authentication request including encrypted personal identification information and apparatus identification information, and
said authentication apparatus further comprises a decrypting means for decrypting said personal identification information and said apparatus identification information included in said received

authentication request.

95. An authentication apparatus as set forth in claim 91, wherein said receiving means receives said authentication request further including third
5 identification information used for the charge processing relating to said user.

96. An authentication apparatus as set forth in claim 91, further comprising a charge processing means for performing charge processing for the authentication
10 relating to said transaction.

97. A processing apparatus for requesting authentication relating to a transaction performed via a network,

said processing apparatus comprising:

15 a transmitting means for transmitting said authentication request including personal identification information for identifying a user and apparatus identification information for identifying a related processing apparatus,
20 a receiving means for receiving an authentication reply including identification information for identifying a transmitting apparatus of the authentication request, and

a controlling means for deciding whether or not
25 said personal identification information and the

identification information included in said authentication reply coincide.

98. A processing apparatus as set forth in claim 97, wherein said controlling means sends a predetermined notification to the transmitting side of said authentication reply when deciding that said apparatus identification information and the identification information included in said authentication reply do not coincide.

99. A processing apparatus as set forth in claim 97, wherein said controlling means sends a predetermined notification to the apparatus of the destination of transaction where the result of the related authentication included in said authentication reply is used when deciding that said apparatus identification information and the identification information included in said authentication response do not coincide.

100. An authentication system comprising a processing apparatus and an authentication apparatus connected via a network, wherein

said authentication apparatus comprises:

a receiving means for receiving an authentication request including personal identification information for identifying a user and apparatus

identification information for identifying a transmitting

apparatus of said authentication request,

a storage means for storing said personal
identification information and information of a
transmission destination for transmitting the
5 authentication result in correspondence,

an authentication processing means for
performing authentication processing in response to said
authentication request, and

a transmitting means for reading the
10 information of said transmission destination
corresponding to said personal identification information
included in said authentication request from said storage
means and transmitting an authentication reply including
the result of said authentication processing and said
15 apparatus identification information included in said
authentication request to the transmission destination
specified by the related read transmission destination
information and wherein

said processing apparatus comprises:

20 a transmitting means for transmitting said
authentication request including said personal
identification information and said apparatus
identification information for identifying the related
processing apparatus,

25 a receiving means for receiving said

authentication reply, and

a controlling means for deciding whether or not
said apparatus identification information of the related
processing apparatus and said apparatus identification
5 information included in said authentication reply
coincide.

101. An authentication method using a processing
apparatus and an authentication apparatus connected via a
network,

10 said authentication method comprising the steps
of:

transmitting an authentication request
including personal identification information for
identifying a user and apparatus identification
15 information for identifying a related processing
apparatus from said processing apparatus to said
authentication apparatus,

performing authentication processing in
response to said authentication request at said
20 authentication apparatus,

transmitting an authentication reply including
the result of said authentication processing and said
apparatus identification information included in said
authentication request to said processing apparatus
25 specified by the information of said transmission

2025110 2626660

destination corresponding to said personal identification information included in said authentication request from said authentication apparatus, and

5 having said processing apparatus decide whether
or not said apparatus identification information included
in said authentication reply received from said
authentication apparatus, said apparatus identification
information of the related processing apparatus, and said
apparatus identification information included in said
10 authentication reply coincide.

102. An authentication method as set forth in claim
101, wherein said processing apparatus sends a
predetermined notification to said authentication
apparatus when deciding that the identification
15 information included in said authentication reply does
not coincide.

103. An authentication method as set forth in claim
101, wherein said processing apparatus sends a
predetermined notification to the apparatus of the
20 destination of transaction where the result of said
authentication included in said authentication reply is
used when deciding that the identification information
included in said authentication reply does not coincide.

104. An information storage method comprising of the
25 steps of

2057140 4644660

dividing predetermined information into a plurality of modules each independently maintaining confidentiality of the predetermined information and

storing said plurality of modules on storage media different from each other or in different regions of an identical storage medium.

105. An information restoration method comprising the steps of:

reading modules from a plurality of storage media or different regions of an identical storage medium when a plurality of modules each independently maintaining confidentiality of the predetermined information are stored on a plurality of storage media different from each other or in different regions of an identical storage medium and

combining the related read modules to restore said predetermined information.

106. An information restoration method as set forth in claim 105, wherein the plurality of storage media different from each other and with said plurality of modules stored therein are storage media physically independent from each other.

107. An information restoration method as set forth in claim 105, wherein said read modules are combined and then decrypted to restore said predetermined information.

108. An information storage device comprising
an information dividing means for dividing said
predetermined information into a plurality of modules
each independently maintaining the confidentiality of the
5 predetermined information and

a writing means for writing said plurality of
modules on storage media different from each other or in
different regions of an identical storage medium.

109. An information storage device as set forth in
10 claim 108, wherein said plurality of storage media
different from each other on which the plurality of
modules are stored are storage media physically
independent from each other.

110. An information storage device as set forth in
15 claim 108, wherein

said device further comprises an encrypting
means for encrypting said predetermined information and

said information dividing means divides the
information obtained by the encryption into said
20 plurality of modules each independently maintaining the
confidentiality of the predetermined information.

111. An information storage device as set forth in
claim 108, wherein

said device further comprises an encrypting
25 means for encrypting said plurality of modules and

0993797 011502

said writing means writes the plurality of modules obtained by the encryption in storage media different from each other or in different regions of an identical storage medium.

5 112. An information restoration device comprising
a reading means for reading modules from a plurality of storage media or different regions of an identical storage medium when a plurality of modules each independently maintaining the confidentiality of the
10 predetermined information are stored on a plurality of storage media different from each other or in the different regions of the identical storage medium and
an information combining means for combining the related read modules to restore said predetermined
15 information.

113. An information restoration device as set forth in claim 112, wherein said plurality of storage media different from each other on which the plurality of modules are stored are storage media physically
20 independent from each other.

114. An information restoration device as set forth in claim 112, further comprising a decrypting means for decrypting the information obtained by combining the modules.

25 115. An information restoration device as set forth

in claim 112, wherein

said device further comprises a decrypting
means for decrypting said read modules and

said information combining means combines said
5 decrypted modules to restore said predetermined
information.

116. A computer readable storage medium storing one
module among a plurality of modules when predetermined
information is divided into a plurality of modules each
10 independently maintaining the confidentiality of the
predetermined information.

2025740" 45445500

MARKED UP VERSION SHOWING CANCELLATION OF CLAIMS

- 1 -

CLAIMS

1. An authentication apparatus for authenticating a transaction performed between at least two parties via a network,

5 said authentication apparatus comprising:

a first receiving means for receiving a first request including personal key information of a first transactor and information indicating a transaction content from said first transactor,

10 a first authenticating means for authenticating a legitimacy of said first transactor based on said personal key information included in said first request and generating first authentication information,

a first transmitting means for transmitting a
15 second request including information obtained by deleting the personal key information of said first transactor from said first request and said first authentication information to said second transactor,

a second receiving means for receiving a reply
20 with respect to said second request from said second transactor,

a second authenticating means for authenticating the legitimacy of said second transactor and generating second authentication information in
25 accordance with said reply, and

a second transmitting means for transmitting
said second authentication information to said first
transactor.

2. ~~An authentication apparatus as set forth in~~
5 ~~claim 1, wherein said personal key information of said~~
~~first transactor is information relating to the charging~~
~~of said first transactor.~~

3. ~~An authentication apparatus as set forth in~~
claim 1, further comprising a storage means for storing
10 ~~log information indicating a log of said transaction.~~

4. An authentication system for authenticating a
transaction performed between at least two parties via a
network,

said authentication system comprising:

15 a first communication apparatus used by a first
transactor,

a second communication apparatus used by a
second transactor, and

an authentication apparatus for authenticating
20 said transaction,

wherein

said authentication apparatus comprises

a first receiving means for receiving a first
request including personal key information of the first
25 transactor and information indicating transaction content

from said first transactor,

a first authenticating means for authenticating
a legitimacy of said first transactor based on said
personal key information included in said first request
5 and generating first authentication information,

a first transmitting means for transmitting a
second request including information obtained by deleting
the personal key information of said first transactor
from said first request and said first authentication
10 information to said second transactor,

a second receiving means for receiving a reply
with respect to said second request from said second
transactor,

a second authenticating means for
15 authenticating the legitimacy of said second transactor
and generating second authentication information in
accordance with said reply, and

a second transmitting means for transmitting
the second authentication information indicating the
20 legitimacy of said transaction to said first transactor.

5. An authentication method for authenticating a
transaction performed between at least two parties via a
network,

said authentication method comprising the steps
25 of:

receiving a first request including personal key information of a first transactor and information indicating transaction content from said first transactor,

5 authenticating a legitimacy of said first transactor based on said personal key information included in said first request and generating first authentication information,

transmitting a second request including
10 information obtained by deleting the personal key information of said first transactor from said first request and said first authentication information to said second transactor,

receiving a reply with respect to said second
15 request from said second transactor,

authenticating a legitimacy of said second transactor in accordance with said reply and generating second authentication information, and

transmitting said second authentication
20 information to said first transactor.

~~6. An authentication method as set forth in claim 5, wherein said transaction is settled using the personal key information of said first transactor.~~

7. An authentication apparatus for authenticating
25 a transaction performed between at least two parties via

03937797 011502

a network,

said authentication apparatus comprising:

a first receiving means for receiving a first request including personal identification information of
5 a first transactor and information indicating transaction content from said first transactor,

a first authenticating means for authenticating a legitimacy, of said first transactor and generating a first authentication information in response to said
10 first request,

a first transmitting means for transmitting a second request including said first authentication information and information indicating content of said transaction to a second transactor,

15 a second receiving means for receiving a reply with respect to said second request from said second transactor,

a second authenticating means for authenticating a legitimacy of said second transactor in
20 accordance with said reply and generating second authentication information, and

a second transmitting means for transmitting said second authentication information to said first transactor.

25 8. An authentication apparatus as set forth in

claim 7, wherein

said first receiving means receives said first request further including the personal key information of said first transactor, and

5 said first authenticating means authenticates the legitimacy of said first transactor based on said personal key information.

9. An authentication apparatus as set forth in claim 8, wherein said personal key information of said
10 first transactor is information relating to the charging of said first transactor.

10. An authentication apparatus as set forth in claim 9, wherein said first transmitting means transmits the second request further including said personal key
15 information of said first transactor to said second transactor.

~~11. An authentication apparatus as set forth in claim 7, further comprising a storage means for storing log information indicating a log of said transaction.~~

20 12. An authentication apparatus as set forth in claim 7, further comprising a decrypting means for decrypting said received first request when said first request is encrypted.

25 13. An authentication apparatus as set forth in claim 7, further comprising an encrypting means for

encrypting said second request.

14. An authentication apparatus as set forth in claim 7, further comprising a decrypting means for decrypting said received reply when said reply is encrypted.

15. An authentication apparatus as set forth in claim 7, further comprising an encrypting means for encrypting said second authentication information.

16. An authentication system for authenticating a transaction performed between at least two parties via a network,

said authentication system comprising:

a first communication apparatus used by a first transactor,

a second communication apparatus used by a second transactor, and

an authentication apparatus for authenticating said transaction,

wherein

said first communication apparatus transmits a first request including personal identification information of the first transactor and information indicating the transaction content to said authentication apparatus, and

said authentication apparatus comprises:

a first receiving means for receiving said
first request from said first transactor,

a first authenticating means for authenticating
a legitimacy of said first transactor and generating
5 first authentication information in response to said
first request,

a first transmitting means for transmitting a
second request including said first authentication
information and the content of said transaction to said
10 second transactor,

a second receiving means for receiving a reply
with respect to said second request from said second
transactor,

a second authenticating means for
15 authenticating a legitimacy of said second transactor and
generating second authentication information in response
to said reply, and

a second transmitting means for transmitting
said second authentication information to said first
20 transactor.

~~17. An authentication system as set forth in claim
16, wherein~~

~~_____ said first receiving means receives said first
request further including personal key information of
25 said first transactor and~~

~~_____ said first authenticating means authenticates
the legitimacy of said first transactor based on said
personal key information.~~

18. ~~An authentication system as set forth in claim
5 17, wherein said personal key information of said first
transactor is information relating to charging of said
first transactor.~~

19. An authentication method for authenticating a
transaction performed between at least two parties via a
10 network,

said authentication method comprising the steps
of:

receiving a first request including personal
identification information of a first transactor and
15 information indicating transaction content from said
first transactor,

authenticating a legitimacy of said first
transactor and generating first authentication
information in response to said first request,

20 transmitting a second request including said
first authentication information and the content of said
transaction to a second transactor,

receiving a reply with respect to said second
request from said second transactor,

25 authenticating a legitimacy of said second

transmitting said second authentication
information to said first transactor.

~~receiving said first request further including~~
~~personal key, information of said first transactor and~~
~~authenticating the legitimacy of said first~~
~~transactor based on said personal key information.~~

~~22. An authentication method as set forth in claim 21, further comprising the step of sending a second request further including said personal key information of said first transactor to said second transactor.~~

24. An authentication apparatus holding information relating to a first transactor and authenticating a transaction between said first transactor and a second

transactor performed via a network while communicating with another authentication apparatus holding information relating to said second transactor,

said authentication apparatus comprising:

5 a transmitting and receiving means for transmitting a second request including information specifying said second transactor in response to a first request from, said first transactor including information indicating said transaction content and information
10 specifying said second transactor to said second authentication apparatus, receiving first signature information indicating an authentication result by said second authentication apparatus in response to said second request, transmitting a third request including
15 information relating to said transaction content included in said first request and said first signature information to an apparatus used by said second transactor, and receiving a predetermined reply from an apparatus used by said second transactor in response to
20 the related third request,

a storage means for storing a log of said transaction when receiving said predetermined reply, and

a signature producing means for producing second signature information to be transmitted to the
25 apparatus used by said first transactor via said

transmitting and receiving means when receiving said predetermined reply and indicating the authentication result of the legitimacy of said transaction.

25. An authentication apparatus as set forth in
5 claim 24, further comprising an encrypting means, and
wherein

said transmitting and receiving means receives
an encryption key used for the communication with said
second transactor from said other authentication
10 apparatus in response to said second request and
transmits the information relating to said transaction
content encrypted by using said encryption key at said
encrypting means and said first signature information to
the apparatus used by said second transactor.

15 26. An authentication apparatus as set forth in
claim 24, wherein

said transmitting and receiving means receives
said predetermined reply including the identification
information used for identifying said second transactor
20 by said other authentication apparatus from the apparatus
used by said second transactor, and

said storage means stores a log of said
transactions generated by using said identification
information.

25 27. An authentication apparatus as set forth in

claim 24, wherein said transmitting and receiving means transmits the third request including information other than the information relating to the charging of said first transactor in the information relating to said transaction content included in said first request and said first signature information to the apparatus used by said second transactor.

28. An authentication apparatus as set forth in claim 24, wherein said transmitting and receiving means transmits the third request including the information relating to said transaction content included in said first request, said first signature information, and the encryption key used for the communication with the related authentication apparatus to the apparatus used by said second transactor.

29. An authentication apparatus as set forth in claim 24, further comprising a charge processing means for the charge processing for the authentication relating to said transaction.

30. An authentication apparatus as set forth in claim 24, wherein said charge processing means performs processing for determining a rate of the charge for the authentication relating to said transaction with said other authentication apparatus.

31. An authentication apparatus as set forth in

claim 24, wherein said transmitting and receiving means receives said predetermined reply from the apparatus used by said second transactor when said second transactor confirms the legitimacy of said first signature
5 information and agrees to the related transaction.

32. An authentication apparatus as set forth in claim 24, wherein said receiving means sends said second signature information to the apparatus used by said second transactor.

10 33. An authentication system for authenticating a transaction performed between at least two parties via a network,

said authentication system comprising:

a first authentication apparatus for
15 authenticating a transaction relating to a first transactor and

a second authentication apparatus for authenticating a transaction relating to a second transactor,

20 wherein

said first authentication apparatus transmits a second request including information specifying said second transactor to said second authentication apparatus in response to a first request by said first transactor
25 including information indicating said transaction content

and information specifying said second transactor,
receives first signature information from said second
authentication apparatus in response to said second
request, transmits a third request including information
5 relating to said transaction content included in said
first request and said first signature information to the
apparatus used by said second transactor, stores a log of
said transaction when receiving a predetermined reply
from said second transactor in response to the related
10 third request, and provides second signature information
for authenticating a legitimacy of said transaction to
said first transactor.

~~34. An authentication system as set forth in claim
33, further comprising an encrypting means, and
15 _____ wherein
_____ said transmitting and receiving means receives
an encryption key used for communication with said second
transactor from said second authentication apparatus in
response to said second request and transmits information
20 relating to said transaction content encrypted by using
said encryption key at said encrypting means and said
first signature information to the apparatus used by said
second transactor.~~

~~35. An authentication system as set forth in claim
25 33, wherein~~

~~_____ said transmitting receiving means of said first authentication apparatus receives said predetermined reply including identification information for use by said second authentication apparatus for identifying said second transactor from said second transactor and _____ said storage means stores said transaction log generated using said identification information.~~

36. ~~An authentication system as set forth in claim 33, wherein said first authentication apparatus provides said second signature information to said second transactor.~~

37. An authentication method for authenticating a transaction between a first transactor and a second transactor performed via a network by using a first authentication apparatus for authenticating a transaction relating to the first transactor and a second authentication apparatus for authenticating a transaction relating to the second transactor,

said authentication method comprising the steps of:

issuing a first request including information indicating said transaction content and information specifying said second transactor from said first transactor to said first authentication apparatus,

transmitting a second request including the

information specifying said second transactor from said first authentication apparatus to said second authentication apparatus in response to said first request,

5 transmitting first signature information indicating the authentication result by the related second authentication apparatus to said first authentication apparatus from said second authentication apparatus in response to said second request,

10 transmitting a third request including the information relating to said transaction content included in said first request and said first signature information from said first authentication apparatus to an apparatus used by said second transactor,

15 issuing a predetermined reply from the apparatus used by said second transactor to said first authentication apparatus in response to the related third request and,

 in accordance with said predetermined reply,
20 storing a log of said transaction, producing second signature information indicating the authentication result of the legitimacy of said transaction, and transmitting the related second signature information to the apparatus used by said first transactor by said first
25 authentication apparatus.

38. An authentication method as set forth in claim 37, further comprising the steps of:

5 sending an encryption key for use in communication with said second transactor from said second authentication apparatus to said first authentication apparatus in accordance with said second request and

10 having said first authentication apparatus encrypt said information relating to transaction content and said first signature information using said encryption key, then send them to the apparatus used by said second transactor.

39. An authentication method as set forth in claim 37, further comprising the steps of having said first authentication apparatus receive said predetermined reply including identification information for use by said second authentication apparatus in identifying said second transactor from the apparatus used by said second transactor and store a log of said transaction generated using said identification information.

40. An authentication method as set forth in claim 37, further comprising the steps of sending a third request including information other than the information relating to the charging of said first transactor in the information relating to said transaction content included

in said first request and said first signature information from the first authentication apparatus to the apparatus used by said second transactor.

41. An authentication method as set forth in claim
5 37, further comprising the steps of sending a third request including information relating to the charging of said first transactor included in said first request, said first signature information, and an encryption key for use in communication with said authentication
10 apparatus from the first authentication apparatus to the apparatus used by said second transactor.

~~42. An authentication method as set forth in claim
37, further comprising the steps of performing processing for determining a rate of charging for authentication
15 relating to said transaction between said first authentication apparatus and said second authentication apparatus.~~

~~43. An authentication method as set forth in claim
37, further comprising the steps of sending said
20 predetermined reply from the apparatus used by said second transactor to said first authentication apparatus when said second transactor confirms the legitimacy of said first signature information and agrees to the related transaction.~~

25 ~~44. An authentication method as set forth in claim~~

~~37, further comprising the steps of sending said second signature information from said first authentication apparatus to the apparatus used by said second transactor.~~

5 45. An authentication method for authenticating a transaction between a first transactor and a second transactor performed via a network by using a first authentication apparatus for authenticating a transaction relating to the first transactor and a second
10 authentication apparatus for authenticating a transaction relating to the second transactor,

 said authentication method comprising the steps of:

 issuing a first request including information
15 indicating said transaction content, personal key information of said first transactor, and information specifying said second transactor from said first transactor to said first authentication apparatus,
 transmitting a second request obtained by
20 deleting said personal key from said first request from said first authentication apparatus to said second authentication apparatus in response to said first request,

 transmitting a third request including
25 information indicating the content of said transaction

from said second authentication apparatus to the
apparatus used by said second transactor in response to
said second request,

transmitting a first reply from the apparatus
5 used by said second transactor to said second
authentication apparatus in response to said third
request,

transmitting a second reply including payment
method information indicating a payment method to said
10 second transactor from said second authentication
apparatus to said first authentication apparatus in
accordance with said first reply, and

managing a payment relating to said transaction
between said first transactor and said second transactor
15 based on said payment method information by said first
authentication apparatus.

46. An authentication method as set forth in claim
45, wherein said first authentication apparatus performs
processing for receiving a payment from said first
20 transactor relating to said transaction, processing for
paying a part of said payment to said second transactor
in accordance with said transaction, and processing for
receiving a remainder of said payment as a fee.

47. An authentication method as set forth in claim
25 45, wherein said first authentication apparatus inquires

to said second authentication apparatus whether or not
said second transactor has contracted with said second
authentication apparatus in response to said first
request and, when receiving an answer indicating it has
5 contracted with it from said second authentication
apparatus, transmits said second request to said second
authentication apparatus.

48. An authentication method as set forth in claim
45, wherein when receiving said second reply, said first
10 authentication apparatus transmits a third reply
including signature information including the result of
authentication performed by the related first
authentication apparatus for said transactor to the
apparatus used by said first transactor.

15 ~~49. An authentication method as set forth in claim
45, wherein said first authentication apparatus encrypts
said third reply by using a secret key corresponding to
the related first authentication apparatus and transmits
the same to the apparatus used by said first transactor.~~

20 ~~50. An authentication method as set forth in claim
45, wherein said first authentication apparatus transmits
said second request further including the signature
information indicating the result of authentication
performed by the related first authentication apparatus
25 for said transaction to said second authentication~~

apparatus.

51. ~~An authentication method as set forth in claim~~
~~45, wherein said second authentication apparatus~~
~~transmits said third request further including signature~~
5 ~~information indicating the result of authentication~~
~~performed by the related second authentication apparatus~~
~~for said transaction to the apparatus used by said second~~
~~transactor.~~ ,

52. ~~An authentication method as set forth in claim~~
10 ~~45, wherein said first authentication apparatus encrypts~~
~~said second request by using a secret key corresponding~~
~~to the related first authentication apparatus and~~
~~transmits the same to said second authentication~~
~~apparatus.~~

53. ~~An authentication method as set forth in claim~~
15 ~~45, wherein said second authentication apparatus encrypts~~
~~said third request by using a secret key corresponding to~~
~~the related second authentication apparatus and transmits~~
~~the same to the apparatus used by said second transactor.~~

54. ~~An authentication method as set forth in claim~~
20 ~~45, wherein the apparatus of said second transactor~~
~~encrypts said first reply by using a secret key of the~~
~~related second transactor and transmits the same to said~~
~~second authentication apparatus.~~

55. ~~An authentication method as set forth in claim~~
25

~~45, wherein said second authentication apparatus encrypts
said second reply by using a secret key corresponding to
the related second authentication apparatus and transmits
the same to said first authentication apparatus.~~

5 56. An authentication apparatus holding information
relating to a first transactor and authenticating a
transaction between said first transactor and a second
transactor performed via a network while communicating
with another authentication apparatus holding information
10 relating to said second transactor,

 said authentication apparatus comprising:

 a receiving means for receiving a first request
including information indicating said transaction
content, personal key information of said first
15 transactor, and information specifying said second
transactor from said first transactor and receiving a
reply including payment method information indicating a
payment method to said second transactor from said other
authentication apparatus,

20 a transmitting means for transmitting a second
request obtained by deleting said personal key from said
first request to said other authentication apparatus in
response to said first request, and

 a charging means for managing a payment
25 relating to said transaction between said first

transactor and said second transactor based on said payment method information.

57. An authentication apparatus as set forth in claim 56, wherein said charging means performs processing for receiving a payment from said first transactor relating to said transaction, processing for paying a part of said payment to said second transactor in accordance with said transaction, and processing for receiving a remainder of said payment as a fee.

58. An authentication apparatus as set forth in claim 56, wherein said transmitting means inquires to said other authentication apparatus whether or not said second transactor has contracted with said second authentication apparatus in response to said first request and, when receiving an answer indicating it has contracted with it from said other authentication apparatus, transmits said second request to said other authentication apparatus.

59. An authentication apparatus as set forth in claim 56, wherein when said receiving means receives said second reply, said transmitting means transmits a reply including signature information including the result of authentication performed by itself for said transactor to the apparatus used by said first transactor.

60. An authentication apparatus as set forth in

claim 59, wherein said transmitting means encrypts said reply by using a secret key corresponding to the related first authentication apparatus and transmits the same to the apparatus used by said first transactor.

5 61. An authentication apparatus as set forth in claim 56, wherein said transmitting means transmits said second request further including the signature information indicating the result of authentication performed by the related first authentication apparatus
10 for said transaction to said other authentication apparatus.

2057110 456/5550
15 62. An authentication system comprising a first authentication apparatus for authenticating a transaction relating to a first transactor and a second authentication apparatus for authenticating a transaction relating to a second transactor and authenticating a transaction between said first transactor and said second transactor performed via a network,

20 said authentication system comprising the steps of:

 issuing a first request including information indicating said transaction content, personal key information of said first transactor, and information specifying said second transactor from said first
25 transactor to said first authentication apparatus,

transmitting a second request obtained by deleting said personal key from said first request from said first authentication apparatus to said second authentication apparatus in response to said first request,

transmitting a third request including the information indicating the content of said transaction from said second authentication apparatus to the apparatus used by said second transactor in response to said second request,

transmitting a first reply from an apparatus used by said second transactor to said second authentication apparatus in response to said third request,

transmitting a second reply including payment method information indicating a payment method to said second transactor from said second authentication apparatus to said first authentication apparatus in accordance with said first reply, and

managing a payment relating to said transaction between said first transactor and said second transactor based on said payment method information by said first authentication apparatus.

~~63. An authentication system as set forth in claim 62, wherein said first authentication apparatus performs~~

~~processing for receiving a payment from said first
transactor relating to said transaction, processing for
paying a part of said payment to said second transactor
in accordance with said transaction, and processing for
5 receiving a remainder of said payment as a fee.~~

~~64. An authentication system as set forth in claim
62, wherein said first authentication apparatus inquires
to said second authentication apparatus whether or not
said second transactor has contracted with said second
10 authentication apparatus in response to said first
request and, when receiving an answer indicating it has
contracted with it from said second authentication
apparatus, transmits said second request to said second
authentication apparatus.~~

~~65. An authentication system as set forth in claim
62, wherein when receiving said second reply, said first
authentication apparatus transmits a third reply
including signature information including the result of
authentication performed by the related first
20 authentication apparatus for said transactor to the
apparatus used by said first transactor.~~

~~66. An authentication system as set forth in claim
62, wherein said first authentication apparatus encrypts
said third reply by using a secret key corresponding to
25 the related first authentication apparatus and transmits~~

~~the same to the apparatus used by said first transactor.~~

~~67. An authentication system as set forth in claim
62, wherein said first authentication apparatus transmits
said second request further including the signature
5 information indicating the result of authentication
performed by the related first authentication apparatus
for said transaction to said second authentication
apparatus.~~

~~68. An authentication system as set forth in claim
10 62, wherein said second authentication apparatus
transmits said third request further including signature
information indicating the result of authentication
performed by the related second authentication apparatus
for said transaction to the apparatus used by said second
15 transactor.~~

~~69. An authentication system as set forth in claim
62, wherein said first authentication apparatus encrypts
said second request by using a secret key corresponding
to the related first authentication apparatus and
20 transmits the same to said second authentication
apparatus.~~

~~70. An authentication system as set forth in claim
62, wherein said second authentication apparatus encrypts
said third request by using a secret key corresponding to
25 the related second authentication apparatus and transmits~~

~~the same to the apparatus used by said second transactor.~~

~~71. An authentication system as set forth in claim
62, wherein the apparatus of said second transactor
encrypts said first reply by using a secret key of the
5 related second transactor and transmits the same to said
second authentication apparatus.~~

~~72. An authentication system as set forth in claim
62, wherein said second authentication apparatus encrypts
said second reply by using a secret key corresponding to
10 the related second authentication apparatus and transmits
the same to said first authentication apparatus.~~

73. An authentication method comprising the steps
of:

having an authentication apparatus divide
15 authentication information of a user into first
authentication information and second authentication
information,

providing a portable memory device storing said
second authentication information to said user,

20 transmitting an authentication information
request from a terminal capable of accessing said
portable memory device to said authentication apparatus,

transmitting said first authentication
information from said authentication apparatus to said
25 terminal when said authentication apparatus decides said

authentication information request is by a legitimate user, and

having said terminal restore said authentication information by using said first authentication information received from said authentication apparatus and said second authentication information read from said portable memory device.

~~74. An authentication method as set forth in claim 73, wherein~~

~~10 said authentication information request includes transmission destination information designating a destination of transmission of said first authentication information, and~~
~~said authentication apparatus transmits said~~
~~15 first authentication information to said terminal designated by said transmission destination information.~~

~~75. An authentication method as set forth in claim 73, wherein said authentication apparatus stores transmission destination information corresponding to~~
~~20 said user in advance and decides that said authentication information request is by the legitimate user when said transmission destination information included in said authentication information request is present in the related stored transmission destination information.~~

~~25 76. An authentication method as set forth in claim~~

~~73, wherein said terminal stores said received first authentication information and restores said authentication information when deciding that said first authentication information received from said authentication apparatus and said second authentication information read from said portable memory device correspond.~~

~~77. An authentication method as set forth in claim 73, wherein said terminal transmits to said authentication apparatus a notification indicating that said first authentication information received from said authentication apparatus and said second authentication information read from said portable memory do not correspond when this is the case.~~

~~78. An authentication method as set forth in claim 73, wherein said authentication apparatus generates said authentication information in response to a request from said user.~~

~~79. An authentication method as set forth in claim 73, wherein said authentication information is information produced by using a public key encryption.~~

~~80. An authentication method as set forth in claim 73, wherein said portable memory device is a smart card.~~

81. An authentication method comprising the steps of:

generating authentication information,
dividing said authentication information into
first authentication information and second
authentication information,

5 providing a portable memory device storing said
second authentication information to a user, and

transmitting said first authentication
information to a transmission destination designated by
said authentication information request when deciding
10 that the received authentication information request is
by a legitimate user.

82. An authentication method as set forth in claim
81, further comprising the steps of:

storing in advance transmission destination
15 information corresponding to the user and

deciding that said authentication information
request is by a legitimate user when said transmission
destination information included in said authentication
information request is present in said stored
20 transmission destination information.

83. An authentication method as set forth in claim
81, wherein said authentication information is
information produced using public key encryption.

84. An authentication method as set forth in claim
25 81, wherein said portable memory device is a smart card.

85. An authentication apparatus comprising:

a controlling means for generating authentication information, dividing said authentication information into first authentication information and second authentication information, and deciding whether or not the received authentication information request is by a legitimate user,

a writing means for writing said second authentication information into a portable memory device,

a receiving means for receiving said authentication information request from a user of said portable memory device, and

a transmitting means for transmitting said first authentication information to a transmission destination designated by said authentication information request when it is decided that said authentication information request is by a legitimate user.

86. An authentication apparatus as set forth in claim 85, further comprising

a storage means for storing in advance transmission destination information corresponding to the user is further provided and

wherein

said controlling means decides that said authentication information request is by a legitimate

user when said transmission destination information included in said authentication information request is present in said stored transmission destination information.

5 87. An authentication apparatus as set forth in claim 85, wherein said authentication information is information produced using public key encryption.

10 ~~88. An authentication apparatus as set forth in claim 85, wherein said portable memory device is a smart card.~~

 89. A communication apparatus comprising:
 a receiving means for receiving a request including personal identification information for identifying a user,
15 a storage means for storing said personal identification information and information of a transmission destination for transmitting a processing result in correspondence,
 a processing means for performing predetermined
20 processing in response to said request, and
 a transmitting means for reading information of said transmission destination corresponding to said personal identification information included in said request from said storage means and transmitting the
25 result of said processing to the transmission destination

specified by the related read information of said transmission destination.

90. A communication apparatus as set forth in claim 89, wherein

5 said receiving means receives a request including encrypted personal identification information, and

 said communication apparatus further comprises a decrypting means for decrypting said personal
10 identification information included in said received request.

91. A communication apparatus as set forth in claim 89, wherein said personal identification information is an identifier assigned to the user registered in the
15 communication apparatus in advance.

92. A communication apparatus as set forth in claim 89, wherein the information of the transmission destination for transmitting the result of said processing is information provided by the transmitting
20 side of said request to the related communication apparatus off-line.

93. A communication apparatus as set forth in claim 89, wherein the information of the transmission destination for transmitting said predetermined result is
25 personal identification information for unambiguously

identifying said user in the network with the related communication apparatus connected thereto.

94. A communication apparatus as set forth in claim 89, wherein said processing is authentication processing.

5 95. A communication system comprising
 a first communication apparatus and
 a second communication apparatus connected via
a network, wherein
 said first communication apparatus comprises:
10 a first receiving means for receiving a request
including personal identification information for
identifying a user,
 a storage means for storing said personal
identification information and information of a
15 transmission destination for transmitting a processing
result in correspondence,
 a processing means for performing predetermined
processing in response to said request, and
 a first transmitting means for reading the
20 information of said transmission destination
corresponding to said personal identification information
included in said request from said storage means and
transmitting the result of said processing to the
transmission destination specified by the related read
25 information of said transmission destination and wherein

said second communication apparatus comprises:

a second transmitting means for transmitting
said request to said first communication apparatus,

a second receiving means for receiving the
5 result of said processing from said first communication
apparatus, and

an outputting means for outputting the result
of the related received authentication processing.

96. ~~A communication apparatus as set forth in claim~~
10 ~~95, wherein~~

~~----- said first receiving means of said first~~
~~communication apparatus receives said request including~~
~~encrypted personal identification information, and~~

~~----- said first communication apparatus further~~
15 ~~comprises a decrypting means for decrypting said personal~~
~~identification information included in said received~~
~~request.~~

97. ~~A communication apparatus as set forth in claim~~
~~95, wherein said personal identification information is~~
20 ~~an identifier assigned to the user registered in the~~
~~first communication apparatus in advance.~~

98. ~~A communication apparatus as set forth in claim~~
~~95, wherein the information of the transmission~~
~~destination for transmitting the result of said~~
25 ~~processing is information provided by the user of said~~

~~second communication apparatus to the related first
communication apparatus off-line.~~

99. ~~A communication apparatus as set forth in claim
95, wherein the information of the transmission
5 destination for transmitting said predetermined result is
personal identification information for unambiguously
identifying said user in the network with the related
first communication apparatus connected thereto.~~

100. A communication method using a first
10 communication apparatus and a second communication
apparatus connected via a network,
said communication method comprising the steps
of:

transmitting a request including personal
15 identification information for identifying a user from
said second communication apparatus to said first
communication apparatus,

having said first communication apparatus
perform predetermined processing in response to said
20 request, and

having said first communication apparatus refer
to a correspondence of said personal identification
information and information of a transmission destination
for transmitting the result of the processing produced in
25 advance and transmit a result of said processing to the

transmission destination specified by information of the transmission destination corresponding to said personal identification information included in said request.

101. A communication method as set forth in claim
5 100, further comprising the step of having said second communication apparatus output the results of said processing received from said first communication apparatus. ,

102. A communication method as set forth in claim
10 100, further comprising the step of having said first communication apparatus receive said request including encrypted personal identification information and decrypt said personal identification information included in said received reply.

103. A communication method as set forth in claim
15 100, wherein said personal identification information is an identifier assigned to a user registered at said first communication apparatus in advance.

104. A communication method as set forth in claim
20 100, wherein the information of the transmission destination for transmitting the result of said processing is information provided by the transmitting side of said request to the related first communication apparatus off-line.

25 105. A communication method as set forth in claim

100, wherein the information of the transmission
destination for transmitting said predetermined result is
personal identification information for unambiguously
identifying said user in the network with the related
5 first communication apparatus connected thereto.

106. An authentication apparatus for authenticating
a transaction performed between at least two parties via
a network, ,

said authentication apparatus comprising:

10 a first receiving means for receiving a first
request including personal key information of a first
transactor and information indicating a transaction
content from said first transactor,

15 a first authenticating means for authenticating
a legitimacy of said first transactor based on said
personal key information included in said first request
and generating first authentication information,

20 a first transmitting means for transmitting a
second request including information obtained by deleting
the personal key information of said first transactor
from said first request and including said first
authentication information to a second transactor,

25 a second receiving means for receiving a reply
with respect to said second request from said second
transactor,

a second authenticating means for authenticating a legitimacy of said second transactor and generating second authentication information,

a second transmitting means for transmitting
5 said second authentication information to said first transactor,

an identification information issuing means for issuing transaction identification information when receiving said first request, and

10 a log managing means for managing a log of the reception of said first request, transmission of said second request, and the reception of said reply by using said transaction identification information.

107. An authentication apparatus as set forth in
15 claim 106, wherein said transaction log managing means generates log information for each of the reception of said first request, transmission of said second request, and reception of said reply and stores the related log information relating to said transaction identification
20 information.

108. An authentication apparatus as set forth in claim 106, wherein said transmitting means transmits a second request further including said transaction identification information to said second transactor.

25 109. An authentication apparatus as set forth in

claim 106, wherein said second authenticating means authenticates the legitimacy of said reply based on said transaction identification information included in said reply and said log managed by said transaction log managing means.

110. An authentication apparatus as set forth in claim 106,

further comprising an account processing means for performing the account processing concerned in said transaction, and

wherein

said transaction log managing means stores log information indicating that the account processing is terminated in correspondence with said transaction identification information after the end of said account processing.

111. An authentication apparatus as set forth in claim 106, wherein the personal key information of said first transactor is information relating to the charging of said first transactor.

112. An authentication system for authenticating a transaction performed between at least two parties via a network,

said authentication system comprising

a first communication apparatus used by a first

transactor,

a second communication apparatus used by a
second transactor, and

an authentication apparatus for authenticating
5 said transaction, wherein

said authentication apparatus comprises:

a first receiving means for receiving a first
request including personal key information of said first
transactor and including an information indicating the
10 transaction content from said first transactor,

a first authenticating means for authenticating
a legitimacy of said first transactor based on said
personal key information included in said first request
and generating first authentication information,

15 a first transmitting means for transmitting a
second request including information obtained by deleting
the personal key information of said first transactor
from said first request and including said first
authentication information to said second transactor,

20 a second receiving means for receiving a reply
with respect to said second request from said second
transactor,

a second authenticating means for
authenticating a legitimacy of said second transactor in
25 accordance with said reply and generating second

authentication information,

a second transmitting means for transmitting
said second authentication information to said first
transactor,

5 a transaction identification information
issuing means for issuing transaction identification
information when receiving said first request, and

a transaction log managing means for managing a
log of the reception of said first request, transmission
10 of said second request, and the reception of said reply
by using said transaction identification information.

113. An authentication method for authenticating a
transaction performed between at least two parties via a
network,

15 said authentication method comprising the steps
of:

receiving a first request including personal
key information of a first transactor and including
information indicating a transaction content from said
20 first transactor,

issuing transaction identification information
in accordance with the related reception,

authenticating a legitimacy of said first
transactor based on said personal key information
25 included in said first request and generating first

authentication information,

transmitting a second request including
information obtained by deleting the personal key
information of said first transactor from said first
5 request and including said first authentication
information to said second transactor,

receiving a reply with respect to said second
request from said second transactor,

authenticating a legitimacy of said second
10 transactor in accordance with said reply and generating
second authentication information,

transmitting said second authentication
information to said first transactor, and

managing a log of the reception of said first
15 request, transmission of said second request, and the
reception of said reply by using said transaction log
information.

~~114. An authentication method as set forth in claim~~
~~113, further comprising the step of generating log~~
20 ~~information for each of the reception of said first~~
~~request, transmission of said second request, and the~~
~~reception of said reply and storing the related log~~
~~information in correspondence with said transaction~~
~~identification information.~~

25 ~~115. An authentication method as set forth in claim~~

~~114, further comprising the step of transmitting a second request further including said transaction identification information to said second transactor.~~

~~116. An authentication method as set forth in claim~~

5 ~~114, further comprising the step of authenticating the legitimacy of said reply based on said transaction identification information included in said reply and said log managed by said transaction log managing means.~~

~~117. An authentication method as set forth in claim~~

10 ~~114, further comprising the steps of~~
~~performing the account processing concerned in said transaction and~~
~~storing log information indicating that the account processing is terminated in correspondence with~~
15 ~~said transaction identification information after the end of said account processing.~~

~~118. An authentication method as set forth in claim~~

~~114, further comprising the steps of~~
~~receiving said reply including personal key~~
20 ~~information of said second transactor and~~
~~authenticating the legitimacy of said second transactor based on the personal key information of said second transactor.~~

~~119. An authentication method as set forth in claim~~

25 ~~118, wherein the personal key information of said first~~

00937797.014500

~~transactor is information relating to the charging of
said first transactor and the personal key information of
said second transactor is information relating to the
charging of said second transactor.~~

5 120. A communication control apparatus for
controlling communication processing carried out in a
second communication apparatus on a network in response
to a request, from one or more first communication
apparatuses,

10 said communication control apparatus
comprising:

 a storage means for storing apparatus
identification information for identifying said first
communication apparatus,

15 a transmitting means for transmitting a request
including said apparatus identification information
corresponding to the related first communication
apparatus to said second communication apparatus in
response to the request from said first communication
20 apparatus,

 a receiving means for receiving a reply
including the apparatus identification information for
identifying the transmitting apparatus of said request
from said second communication apparatus, and

25 a controlling means for deciding if said

0993797-01502
202510-2624560

request corresponding to said received reply is by a
legitimate first communication apparatus whose apparatus
identification information is stored in said storage
means based on whether or not said apparatus

5 identification information included in said reply and
said apparatus identification information stored in said
storage means coincide.

121. A communication control apparatus as set forth
in claim 120, wherein said controlling means sends a
10 predetermined notification to said second communication
apparatus when said apparatus identification information
included in said reply and said apparatus identification
information stored in said storage means do not coincide.

122. A communication control apparatus as set forth
15 in claim 120, wherein said controlling means sends a
predetermined notification to an apparatus of the
destination of a transaction where the result of
processing included in said reply is used when said
apparatus identification information included in said
20 reply and said apparatus identification information
stored in said storage means do not coincide.

123. A communication control apparatus as set forth
in claim 120, wherein said transmitting means transmits
said request including personal identification
25 information received from said first communication

apparatus and including said apparatus identification information corresponding to the related first communication apparatus to said second communication apparatus.

5 124. A communication control apparatus as set forth in claim 120, wherein said storage means stores said apparatus identification information received from said first communication apparatus.

10 125. A communication control apparatus as set forth in claim 124, wherein said storage means stores said apparatus identification information received from said first communication apparatus when a power of the related communication control apparatus is turned on.

15 126. A communication control apparatus as set forth in claim 120, wherein said controlling means writes a communication log between said first communication apparatus and said second communication apparatus in said storage means.

20 127. A communication control apparatus as set forth in claim 120, wherein said controlling means transmits the processing result of said second communication apparatus included in said reply to said first communication apparatus of the transmission destination of said request.

25 128. A communication control apparatus as set forth

in claim 120, wherein said controlling means controls the communication so that said first communication apparatus in a stand-by state enters an operating state in accordance with the information received from said
5 receiving means.

129. A communication control apparatus as set forth in claim 120, wherein said controlling means controls the communication between a network to which said first communication apparatus is connected and a network to
10 which said second communication apparatus is connected.

130. A communication control apparatus as set forth in claim 120, wherein said controlling means performs processing as a gateway.

131. A communication control apparatus as set forth
15 in claim 120, wherein said apparatus identification information is an identifier that can unambiguously identify the related communication apparatus assigned by the manufacturer of said first communication apparatus.

132. A communication control apparatus as set forth
20 in claim 120, wherein said personal identification information is an identifier assigned to a registered user in advance.

133. A communication control apparatus as set forth in claim 120, wherein said receiving means receives said
25 reply including the result of authentication processing

performed by said second communication apparatus from
said second communication apparatus.

134. A communication system for controlling at a
communication control apparatus communication relating to
5 processing carried out at a second communication
apparatus on a network in response to a request from one
or more first communication apparatuses, wherein

said communication control apparatus comprises:

a first storage means for storing apparatus
10 identification information for identifying said first
communication apparatus,

a first transmitting means for transmitting a
request including said apparatus identification
information corresponding to the related first
15 communication apparatus and including personal
identification information to said second communication
apparatus in response to the request from said first
communication apparatus,

a first receiving means for receiving a reply
20 including the apparatus identification information for
identifying the transmitting apparatus of said request
from said second communication apparatus, and

a controlling means for deciding if said
request corresponding to said received reply is by a
25 legitimate first communication apparatus whose apparatus

0993797 011500
205110 2622560

identification information is stored in said first
storage means based on whether or not said apparatus
identification information included in said reply and
said apparatus identification information stored in said
5 first storage means coincide and wherein

said second communication apparatus comprises:

a second receiving means for receiving said
request,

10 a second storage means for storing said
request,

a second storage means for storing said
personal identification information and information of a
transmission destination for transmitting a processing
result in correspondence,

15 a processing means for performing predetermined
processing in response to said request, and

a second transmitting means for reading the
information of said transmission destination
corresponding to said personal identification information
20 included in said request from said second storage means
and transmitting the result of said processing and said
apparatus identification information included in said
request in correspondence to the transmission destination
specified by the related read transmission destination
25 information.

135. A communication method for controlling at the communication control apparatus communication relating to processing carried out at a second communication apparatus on a network in response to a request from one
5 or more first communication apparatuses,

said communication method comprising the steps of:

transmitting a request including apparatus identification information corresponding to the related
10 first communication apparatus and including personal identification information from said communication control apparatus to said second communication apparatus in response to the request issued from said first communication apparatus to said communication control
15 apparatus,

having said second communication apparatus perform predetermined processing in response to said received request,

having said second communication apparatus
20 transmit a reply including the result of said processing and including said apparatus identification information included in said request to said communication control apparatus based on the information of the transmission destination corresponding to said personal identification
25 information included in said request, and

having said communication control apparatus
decide if said request corresponding to said received
reply is by a legitimate first communication apparatus
based on whether or not said apparatus identification
5 information included in said received reply and said
apparatus identification information of said first
communication apparatus held in advance coincide.

136. A communication method as set forth in claim
135, wherein said communication control apparatus sends a
10 predetermined notification to said second communication
apparatus when said apparatus identification information
included in said received reply and said apparatus
identification information of said first communication
apparatus held in advance do not coincide.

15 ~~137. A communication method as set forth in claim~~
~~135, wherein said communication control apparatus sends a~~
~~predetermined notification to an apparatus of a~~
~~destination of the transaction where the result of~~
~~processing included in the reply is used when said~~
20 ~~apparatus identification information included in said~~
~~received reply and said apparatus identification~~
~~information of said first communication apparatus held in~~
~~advance do not coincide.~~

138. An authentication apparatus for performing
25 authentication processing in response to an

authentication request,

said authentication apparatus comprising:

5 a receiving means for receiving said authentication request including personal identification information for identifying a user and including apparatus identification information for identifying a transmitting apparatus of said authentication request,

10 a storage means for storing said personal identification information and the information of the transmission destination for transmitting an authentication result in correspondence,

an authentication processing means for performing authentication processing in response to said authentication request, and

15 a transmitting means for reading the information of said transmission destination corresponding to said personal identification information included in said authentication request from said storage means and transmitting the result of said authentication processing and said apparatus identification information
20 included in said authentication request in correspondence to the transmission destination specified by the related read transmission destination information.

139. An authentication apparatus as set forth in
25 claim 138, wherein

said receiving means receives said authentication request including encrypted personal identification information and apparatus identification information, and

5 said authentication apparatus further comprises a decrypting means for decrypting said personal identification information and said apparatus identification information included in said received authentication request.

10 140. An authentication apparatus as set forth in claim 138, wherein said receiving means receives said authentication request further including third identification information used for the charge processing relating to said user.

15 141. An authentication apparatus as set forth in claim 138, wherein said personal identification information is an identifier assigned to a registered user in advance.

20 142. An authentication apparatus as set forth in claim 138, wherein said apparatus identification information is an identifier capable of unambiguously identifying the related apparatus assigned by the manufacturer of said apparatus.

25 143. An authentication apparatus for performing authentication processing relating to a transaction

performed via a network,

said authentication apparatus comprising:

a receiving means for receiving an authentication request by a user engaging in a transaction including personal identification information for identifying the user, transaction information indicating content of the transaction, and apparatus identification information for identifying a transmitting apparatus of said authentication request,

a storage means for storing said personal identification information and information of a transmission destination for transmitting the authentication result in correspondence,

an authentication processing means for transmitting said transaction information included in said received authentication request to an apparatus of the user designated by said authentication request and performing predetermined authentication processing in accordance with a reply from the apparatus of the related designated user, and

a transmitting means for reading the information of said transmission destination corresponding to said personal identification information included in said authentication request from said storage means and transmitting the result of said authentication

processing and said apparatus identification information included in said authentication request in correspondence to the transmission destination specified by the related read transmission destination information.

5 144. An authentication apparatus as set forth in claim 143, wherein said authentication processing means attaches signature information indicating the authentication result of the related authentication apparatus to said transaction information and transmits
10 the same to the apparatus of said designated user and generates signature information of the related authentication apparatus of the result of said authentication processing in accordance with the reply from said designated user.

15 145. An authentication apparatus as set forth in claim 143, wherein said storage means stores log information of transactions between the user issuing said authentication request and said designated user.

20 146. An authentication apparatus as set forth in claim 143, wherein

 said receiving means receives said authentication request including encrypted personal identification information and apparatus identification information, and

25 said authentication apparatus further comprises

a decrypting means for decrypting said personal identification information and said apparatus identification information included in said received authentication request.

5 147. An authentication apparatus as set forth in claim 143, wherein said receiving means receives said authentication request further including third identification information used for the charge processing relating to said user.

10 148. An authentication apparatus as set forth in claim 143, further comprising a charge processing means for performing charge processing for the authentication relating to said transaction.

15 149. A processing apparatus for requesting authentication relating to a transaction performed via a network,

 said processing apparatus comprising:

 a transmitting means for transmitting said authentication request including personal identification information for identifying a user and apparatus
20 identification information for identifying a related processing apparatus,

 a receiving means for receiving an authentication reply including identification information
25 for identifying a transmitting apparatus of the

authentication request, and

a controlling means for deciding whether or not
said personal identification information and the
identification information included in said
5 authentication reply coincide.

150. A processing apparatus as set forth in claim
149, wherein said controlling means sends a predetermined
notification, to the transmitting side of said
authentication reply when deciding that said apparatus
10 identification information and the identification
information included in said authentication reply do not
coincide.

151. A processing apparatus as set forth in claim
149, wherein said controlling means sends a predetermined
15 notification to the apparatus of the destination of
transaction where the result of the related
authentication included in said authentication reply is
used when deciding that said apparatus identification
information and the identification information included
20 in said authentication response do not coincide.

152. An authentication system comprising a
processing apparatus and an authentication apparatus
connected via a network, wherein

said authentication apparatus comprises:
25 a receiving means for receiving an

authentication request including personal identification information for identifying a user and apparatus identification information for identifying a transmitting apparatus of said authentication request,

5 a storage means for storing said personal identification information and information of a transmission destination for transmitting the authentication result in correspondence,

10 an authentication processing means for performing authentication processing in response to said authentication request, and

15 a transmitting means for reading the information of said transmission destination corresponding to said personal identification information included in said authentication request from said storage means and transmitting an authentication reply including the result of said authentication processing and said apparatus identification information included in said authentication request to the transmission destination
20 specified by the related read transmission destination information and wherein

 said processing apparatus comprises:

 a transmitting means for transmitting said authentication request including said personal
25 identification information and said apparatus

identification information for identifying the related
processing apparatus,

a receiving means for receiving said
authentication reply, and

5 a controlling means for deciding whether or not
said apparatus identification information of the related
processing apparatus and said apparatus identification
information included in said authentication reply
coincide.

10 ~~153. An authentication system as set forth in claim
152, wherein said processing apparatus sends a
predetermined notification to the transmitting apparatus
of the authentication reply when deciding that the
identification information included in said
15 authentication reply does not coincide.~~

~~154. An authentication system as set forth in claim
152, wherein said processing apparatus sends a
predetermined notification to the apparatus of the
destination of transaction where the result of said
20 authentication included in said authentication reply is
used when deciding that the identification information
included in said authentication reply does not coincide.~~

155. An authentication method using a processing
apparatus and an authentication apparatus connected via a
25 network,

said authentication method comprising the steps
of:

transmitting an authentication request
including personal identification information for
5 identifying a user and apparatus identification
information for identifying a related processing
apparatus from said processing apparatus to said
authentication apparatus,

performing authentication processing in
10 response to said authentication request at said
authentication apparatus,

transmitting an authentication reply including
the result of said authentication processing and said
apparatus identification information included in said
15 authentication request to said processing apparatus
specified by the information of said transmission
destination corresponding to said personal identification
information included in said authentication request from
said authentication apparatus, and

20 having said processing apparatus decide whether
or not said apparatus identification information included
in said authentication reply received from said
authentication apparatus, said apparatus identification
information of the related processing apparatus, and said
25 apparatus identification information included in said

authentication reply coincide.

156. An authentication method as set forth in claim 155, wherein said processing apparatus sends a predetermined notification to said authentication
5 apparatus when deciding that the identification information included in said authentication reply does not coincide.

157. An authentication method as set forth in claim 155, wherein said processing apparatus sends a
10 predetermined notification to the apparatus of the destination of transaction where the result of said authentication included in said authentication reply is used when deciding that the identification information included in said authentication reply does not coincide.

15 158. An information storage method comprising of the steps of

dividing predetermined information into a plurality of modules each independently maintaining confidentiality of the predetermined information and
20 storing said plurality of modules on storage media different from each other or in different regions of an identical storage medium.

~~159. An information storage method as set forth in claim 158, wherein the plurality of storage media
25 different from each other and with said plurality of~~

~~modules stored thereon are storage media physically
independent from each other.~~

~~160. An information storage method as set forth in
claim 158, wherein~~

5 ~~_____ said predetermined information is encrypted,
and~~

~~_____ the information obtained by the related
encryption is divided into said plurality of modules each
independently maintaining the confidentiality of the
10 predetermined information.~~

~~161. An information storage method as set forth in
claim 158, wherein~~

~~_____ said plurality of modules are encrypted, and
_____ the plurality of modules obtained by the
15 encryption are stored on storage media different from
each other or in different regions of an identical
storage medium.~~

~~162. An information restoration method comprising
the steps of:~~

20 ~~reading modules from a plurality of storage
media or different regions of an identical storage medium
when a plurality of modules each independently
maintaining confidentiality of the predetermined
information are stored on a plurality of storage media
25 different from each other or in different regions of an~~

identical storage medium and

combining the related read modules to restore
said predetermined information.

163. An information restoration method as set forth
5 in claim 162, wherein the plurality of storage media
different from each other and with said plurality of
modules stored therein are storage media physically
independent from each other.

164. An information restoration method as set forth
10 in claim 162, wherein said read modules are combined and
then decrypted to restore said predetermined information.

~~165. An information restoration method as set forth
in claim 162, wherein said read modules are decrypted and
then combined to restore said predetermined information.~~

15 166. An information storage device comprising
an information dividing means for dividing said
predetermined information into a plurality of modules
each independently maintaining the confidentiality of the
predetermined information and

20 a writing means for writing said plurality of
modules on storage media different from each other or in
different regions of an identical storage medium.

167. An information storage device as set forth in
claim 166, wherein said plurality of storage media
25 different from each other on which the plurality of

0993797-011502
205710-26226660

modules are stored are storage media physically independent from each other.

168. An information storage device as set forth in claim 166, wherein

5 said device further comprises an encrypting means for encrypting said predetermined information and said information dividing means divides the information obtained by the encryption into said plurality of modules each independently maintaining the confidentiality of the predetermined information.

10

169. An information storage device as set forth in claim 166, wherein

 said device further comprises an encrypting means for encrypting said plurality of modules and

15 said writing means writes the plurality of modules obtained by the encryption in storage media different from each other or in different regions of an identical storage medium.

170. An information restoration device comprising

20 a reading means for reading modules from a plurality of storage media or different regions of an identical storage medium when a plurality of modules each independently maintaining the confidentiality of the predetermined information are stored on a plurality of

25 storage media different from each other or in the

different regions of the identical storage medium and
an information combining means for combining
the related read modules to restore said predetermined
information.

5 171. An information restoration device as set forth
in claim 170, wherein said plurality of storage media
different from each other on which the plurality of
modules are stored are storage media physically
independent from each other.

10 172. An information restoration device as set forth
in claim 170, further comprising a decrypting means for
decrypting the information obtained by combining the
modules.

15 173. An information restoration device as set forth
in claim 170, wherein

 said device further comprises a decrypting
means for decrypting said read modules and

 said information combining means combines said
decrypted modules to restore said predetermined
20 information.

 174. A computer readable storage medium storing one
module among a plurality of modules when predetermined
information is divided into a plurality of modules each
independently maintaining the confidentiality of the
25 predetermined information.